REMARKS

Reconsideration and allowance of the above-referenced application are respectfully requested. Claims 1-78 are unchanged and remain pending in the application.

Claims 1, 2 and 7-10 stand rejected under 35 USC 103 in view of U.S. Patent No. 6,584,564 to Olkin in view of U.S. Patent No. 6,233,318 to Picard. This rejection is respectfully traversed.

Claim 1 specifies a method in a unified communications system. The method includes receiving a request for a user interface session to enable a user to leave a message for an identified destination subscriber. The method also includes generating a first prompt enabling the user to select encryption of the message, and generating a second prompt, based on the user selecting encryption of the message, for the user to supply an encryption key. The method also includes causing encryption of the message into an encrypted message based on the encryption key supplied by the user, and outputting the encrypted message to a determined destination based on determined subscriber profile attributes for the identified destination subscriber.

Hence, claim 1 specifies that the unified communications system generates a first prompt that enables a user to select encryption and a second prompt that enables the user to supply an encryption key, eliminating the necessity of any hardware or software modification by the user device.

These and other features are neither disclosed nor suggested in the applied prior art.

As admitted in the Official Action, Olkin fails to teach that the disclosed e-mail system could be implemented in a unified communications system. Moreover, Olkin fails to disclose or

suggest a centralized messaging system that generates prompts that permits a user to supply an encryption key, as claimed.

Olkin describes a secure e-mail system where a sending computer 18 includes encryption software modules 26 (described with respect to Figure 3) that enables a sending user (i.e., "sender") 12 to send a encrypted secure e-mail 14. In particular, sender 12 uses a "Send Securely" command to request transmission of a secure e-mail 14; the sending computer 18 first contacts a security server 24 and provides the security server with various data items (e.g., sender ID, sender password, and receiver ID).

The security server 24 in response authenticates the sender and replies to the sending unit 18 with a unique message key and message identifier for the present e-mail 14. The security server 24 also logs the transaction by storing the message ID, the unique message key, and the receiver ID (see, e.g., col. 3, lines 53-55 and col. 6, lines 39-40).

The sending unit 18 encrypts the e-mail message 14 using the message key supplied by the security server 24; and the sending unit 18 outputs the e-mail 14 to the e-mail destination (see col. 6, lines 41-43 and 62-64). A significant aspect is that "[t]he message body, encrypted or otherwise, is never sent to the security server 24." (Col. 6, lines 42-43).

Hence, Olkin limits server operations to supplying the encryption key, and never supplies the message body to the server. Consequently, Olkin neither discloses nor suggests a user interface session that enables a user to leave a message for a destination subscriber, let alone generating the first prompt enabling the user to select encryption of the message, let alone a second prompt for the user to supply an encryption key, as claimed.

Consequently, the hypothetical combination of Olkin and Picard would neither disclose nor suggest the claimed feature of a unified communications system that: (1) generates a second prompt, based on the user selecting encryption of the message, for the user to supply an encryption key; (2) causing encryption of the message based on the encryption key supplied by the user; or (3) outputs the encrypted message to a determined destination based on determined subscriber profile attributes for the identified destination subscriber.

Rather, the hypothetical combination would at most provide a unified messaging system having a security server that supplies the encryption key. As apparent from the foregoing, such a system would be highly inefficient due to the requirements that the security server stores log data (including the message ID, the unique message key, and the receiver ID) for each and every e-mail message having been encrypted. Moreover, storing all the message keys, message identifiers and receiver identifiers on the security server 24 creates a vulnerability in that the secure e-mails can be decrypted if the security server 24 is compromised such that the log data is stolen by an untrusted source.

Finally, Olkin explicitly requires that the unencrypted message cannot be sent from the local terminal 18 until encryption has been completed, preventing the system of Picard from storing any message until encryption has been completed locally.

Independent claim 1, however, specifies that the encryption key is supplied by the user, enabling (1) messages to be stored on a server prior to encryption, optimizing storage resources in the unified communications system; (2) scalable security by requiring the user to supply the encryption key; and (3) enabling deployment of encryption resources accessible by the unified

communications system without the necessity of encryption resources at the user device (see claim 2), enabling any type of message (e.g., voice, fax, e-mail, pager, etc.) to be encrypted.

For these and other reasons, the rejection of claims 1 and 2 should be withdrawn.

Regarding claim 8, Applicant further traverses the rejection for the same reasons as described above with respect to claim 1: the hypothetical combination of Olkin and Picard would provide no more than a unified communications system having a security server that supplies the decryption key for decrypting the message after having been opened by the receiver computer 16 of the destination user (see, e.g., col. 7, lines 7-25).

There is no disclosure or suggestion that the hypothetical unified communications system discloses or suggests the claimed feature of detecting one of the stored messages that are to be retrieved are, in fact, encrypted, let alone generating a third prompt for the destination subscriber to supply a decryption key, let alone supplying the decryption key and the one stored message to an invoked decryption utility, as claimed.

For these and other reasons, the rejection of claim 8 should be withdrawn.

The rejection of claim 9 is traversed. As apparent from the foregoing, Olkin explicitly specifies that the encrypted e-mail message is delivered to the destination e-mail client device 20 before decryption occurs. There is no dislosure or suggestion for the claimed feature of "outputting the decrypted data file during the second user interface session to the identified destination subscriber, independent of the encryption key matching the decryption key." For these and other reasons, the rejection of claim 9 should be withdrawn.

The rejection of claim 10 is traversed. As described above, Olkin requires that the unencrypted message resides at the client device: a web-based e-mail system relies on a plug-in 26/46a that intercepts the page 72 (or form) containing the various fields of the e-mail that was about to be posted to the e-mail server 22; the software module 26 encrypts the fields in the e-mail to ensure encryption has been performed before posting the form to the e-mail server 22 (see col. 7-16). Hence, the hypothetical combination neither discloses nor suggests the claied request for a user interface session being received according to HTTP protocol, as claimed. For these and other reasons, the rejection of claim 10 should be withdrawn.

Claims 3-5 stand rejected under §103 in view of Olkin, Picard, and U.S. Patent No. 6,356,937 to Montville et al. It is believed these claims are allowable in view of the dependency from claim 1.

Claim 6 stands rejected under 35 USC §103 in view of Olkin, Picard, and U.S. Patent No. 6,671,355 to Spielman et al. As demonstrated by the Statement of Common Ownership below, U.S. Patent No. 6,671,355 to Spielman et al. is not available as a reference under §103(c); hence, this rejection should be withdrawn.

Applicant objects to the Official Action as being incomplete: the claims 11-78 have not been examined on their merits, as required under MPEP 706.02(j) and 707.07(d). Rather, paragraph 14 on page 7 merely specifies that "Claims 11-78 do not teach any new limitations above claims 1-10 and are therefore rejected for the above-mentioned reasons."

This omnibus rejection of claims 11-78 is improper: claims 11, 22, 30, 37, 47, 58, and 68 are independent claims that are distinct from claim 1. As specified in MPEP 707.07(d):

> An omnibus rejection of the claim "on the references and for the reasons of record" is stereotyped and usually not informative and should therefore be avoided. This is especially true where certain claims have been rejected on one ground and other claims on another ground.
>
> A plurality of claims should never be grouped together in a common rejection, unless that rejection is equally applicable to all claims in the group.
>
> (MPEP 707.07(d), Rev. 2, May 2004, at page 700-118).

Therefore, Applicant respectfully requests the next communication from the Patent Office to provide an explicit statutory basis if the claims 11-78 are to be rejected.

Assuming that independent claims 11, 22, 30, 37, 47, 58, and 68 were rejected under 35 USC 103 in view of Olkin and Picard, the rejection is respectfully traversed for the reasons specified above with respect to claims 1 and 8, the comments of which are incorporated in their entirety herein by reference.

STATEMENT OF COMMON OWNERSHIP

At the time the invention claimed in the subject application was made, the subject application 09/756,697 and U.S. Patent No. to 6,671,355 to Spielman et al. were owned by, or subject to an obligation of assignment to, the same entity (Cisco Technology, Inc., of San Jose, California).

CONCLUSION

In view of the above, it is believed this application is and condition for allowance, and such a Notice is respectfully solicited.

To the extent necessary, Applicant petitions for an extension of time under 37 C.F.R. 1.136. Please charge any shortage in fees due in connection with the filing of this paper, including any missing or insufficient fees under 37 C.F.R. 1.17(a), to Deposit Account No. 50-1130, under Order No. 95-456, and please credit any excess fees to such deposit account.

Respectfully submitted,

Leon R. Turkevich
Registration No. 34,035

Customer No. 23164
Date: July 22, 2004